IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA,	)	
	)	
	)	Case No. 1:08-cr-51-SJM
v.	)	
	)	
	)	
ROBERT EUGENE BEATTY	)	

MEMORANDUM OPINION

McLAUGHLIN, SEAN J., District J.,

Defendant Robert Eugene Beatty has been charged in this criminal action with one count of receiving/distributing or attempting to receive/distribute and one count of possessing visual depictions of a minor engaging in sexually explicit conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), respectively. Presently pending before the Court is the Defendant's motion to suppress evidence of contraband taken from his home computer and statements which the Defendant made in connection with that search and seizure. For the reasons set forth below, this motion will be denied.

I. BACKGROUND

The challenged search in this case was conducted pursuant to a warrant obtained by Special Agent Tom Brenneis of the FBI on July 30, 2008. The affidavit in support of the warrant states that, on April 13, 2008, Trooper Robert Pearson of the Pennsylvania State Police conducted an online undercover investigation using the Gnutella network in a "peer-to-peer" (P2P) environment.[1] (Brenneis Affidavit [49-2] at

[1] As the affidavit explains, peer-to-peer file sharing is a "growing phenomenon on the Internet." (Affidavit of Tom Brenneis [49-2] at ¶ 13.) It involves the use of special software which enables individual internet users to link their computers via a network that allows the direct sharing of digital files (*id*.):

> These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the

¶ 21.) Employing a file sharing program known as "Phex,"[2] Trooper Pearson entered "search terms [known] to be utilized by those interested in child pornography" and, in doing so, obtained a list of shared files located on computers attached to the Gnutella network. (*Id*.)

Trooper Pearson's investigation revealed that an individual assigned Internet Protocol (IP) number 76.188.64.82[3] was using the Gnutella network and his/her own

---

> information is first deposited before its [sic] is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to prevent distribution across the Internet. Further, once a file is placed in a shared folder its distribution is dependant only on the machine being turned on and connected to the Internet. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Limewire, one type of P2P software, sets up its searches by keyword. The results of the keyword search are displayed to the user. The user then selects files from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.
>
> 14. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a search for files using a phrase such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed the files he/she wants to download. The file is downloaded directly from the computer hosting the file. The downloaded file is stored in the area previously designated by the user. The downloaded file will remain there until moved or deleted.

(*Id*. at ¶¶ 13-14.) The affidavit further states that, the strength of the Gnutella network is that "it bases all of its file sharing on the Secure Hash Algorithm" (Brenneis Affidavit at ¶ 17), the significance of which is explained in more detail, *infra*, at n. 5.

[2] "Phex" is a "simple file sharing program which allows a user to share and download any type of files from other users on the Gnutella network," regardless of the file sharing software program being run by other users. (Brenneis Affidavit [49-2] at ¶ 20.) Because it is based on Java technology, it is available for many different systems including Windows, MAC, and others. (*Id*.)

[3] As explained in the search warrant affidavit, an Internet Protocol (IP) address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. (Brenneis Affidavit at ¶ 18.) The IP address provides a unique location making it possible for data to be transferred between computers. No two identical IP addresses can operate on the same segment of the Internet simultaneously. (*Id*.)

P2P software to broadcast for download numerous shared files with titles suggestive of child pornography. (Brenneis Affidavit at ¶ 23.) In particular, the affidavit references the titles of eleven files; nearly all of the file names include graphic references to specific sexual acts involving children and/or terms such as "child_sex," "pedofilia," "illegal pedo sex," "incest" or "Lolita." (*Id.*)[4] Trooper Pearson found that the Secured Hash Algorithm ("SHA1")[5] values of these files matched those in a national database of "known child pornography computer files" maintained by the Wyoming Internet Crimes Against Children (ICAC) Task Force. (*Id.*) Further investigation revealed that the Defendant was the subscriber to IP number 76.188.64.82 on the date in question.

Based largely on the foregoing information, Agent Brenneis obtained a warrant to search the Defendant's home. During the course of the search, the Defendant's

---

[4] By way of example only, the Court sets forth below a sample of some of the file names as they are recorded in the affidavit:

* r@ygold - pedo - 13yo brother fucks 11yo sister and sperm inside 61 943 812.mpg

* (Pthc) 14yo Isabel - (Rape and Fuck) (R@ygold) .mpg

* Little young girl hardfucked by me - 7 yrs R@ygold illegal pedo sex.mpg

* (Hussyfan) (pthc) (r@ygold) (babyshivid) Jessica 11yo get fuckt good.mpg

[5] Agent Brenneis' affidavit explains that the Secure Hash Algorithm, also known as the SHA1 hash set, is a "mathematical algorithm that allows for the fingerprinting of files." (Brenneis Affidavit at ¶ 17.) Once a file is located using a software application capable of generating the SHA1 value, that SHA1 value becomes a unique identifier for that particular file. (*Id.*) The SHA1 is termed "secure" because it is "computationally unfeasible to find files (i.e. computer data, in this case child pornography image/movies) which produce the same message digest (SHA1 hash value result)." (*Id.*) Indeed, according to Agent Brenneis' affidavit, "[t]here is no known instance of two different computer files having the same SHA1 hash value." (*Id.*) Because any change to a message in transit will, "with extremely high probability, result in a different message digest, and alteration of the signature," the SHA1 "digital fingerprint" is "more unique to a data file than DNA is to the human body." (*Id.*)

computer was seized and, according to the Government, was later found to contain hundreds of movies depicting minors engaged in sexually explicit activity. On August 4, 2008, several days after the search of his home, the Defendant was interviewed by the FBI and gave incriminating statements. This indictment followed.

II. DISCUSSION

A. *Reasonable Expectation of Privacy*

According to the Government, the overwhelming majority, if not all, of the alleged child pornography movies that were discovered on the Defendant's computer were located in his shared LimeWire folders. Thus, the first issue we must address is whether the Defendant maintained a reasonable expectation of privacy in the files that were obtained as a result of the Government's search.

The Fourth Amendment, which guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and which ensures that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized," U.S. CONST. amend. IV, is a personal right. *Minnesota v. Carter*, 525 U.S. 83, 88 (1998). To claim the protection of the Fourth Amendment, therefore, an individual must demonstrate that he personally has an expectation of privacy in the place searched and that his expectation is reasonable. *Id*. (citing *Rakas v. Illinois*, 439 U.S. 128, 143-44 (1978)).

Here, the Government contends that the Defendant has no reasonable expectation of privacy in the files retrieved from his computer, at least to the extent the files were located in a shared folder. The Government cites *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009), *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008); *United States v. Barrows*, 481 F.3d 1246, 1249 (10th Cir. 2007); *United States v. Brese*, 2008 WL 1376269, at *2 (W.D. Okla. 2008); *United States v. Borowy*, 577 F. Supp. 2d 1133,

1136 (D. Nev. 2008); and *United States v. Meysenburg*, 2009 WL 1090664 (D. Neb. 2009), as supporting the proposition that an individual using peer-to-peer software to share files on his computer cannot claim the protection of the Fourth Amendment relative to those shared files.

The Government's argument would have more force if the Defendant were challenging Trooper Pearson's use of P2P software to remotely access his shared files, but that is not the situation here. As the Defendant points out, the cases cited by the Government generally recognize that law enforcement officers do not violate the Fourth Amendment by using P2P software to remotely access files contained on a defendant's computer that are being shared by the defendant inasmuch as the defendant has no reasonable expectation of privacy regarding the remote accessing of those files. *See Stults*, 575 F.3d at 843 (agent's use of file-sharing program to access child pornography files on the defendant's computer did not constitute an illegal warrantless search where defendant had made those files accessible to others for sharing and thus lacked any reasonable expectation of privacy in files); *Ganoe*, 538 F.3d at 1127 (no illegal warrantless search where agent used LimeWire to access child pornography files on defendant's computer; defendant lacked reasonable expectation of privacy in those files); *Borowy*, 577 F. Supp. 2d at 1136 (same); *Brese*, 2008 WL 1376269 at *1-2 (same); *Meysenburg*, 2009 WL 1090664 at *2 (rejecting defendant's claim that his privacy interests were violated by officer's use of Phex software to remotely locate child pornography on defendant's computer; court found no support for defendant's factual contention that he had previously disabled his file-sharing program). *Accord Perrine*, 518 F.3d at 1205 (10th Cir. 2008) (defendant, who utilized peer-to-peer software so as to allow other internet users to access at least certain folders in his computer had no reasonable expectation of privacy in the subscriber information given to his internet

provider).[6]

However, none of the cases cited by the Government stand for the proposition that an individual running P2P software thereby loses his Fourth Amendment "standing" [7] to challenge a search which involves entry into his home and the seizure and subsequent search of his entire computer.[8] Were that the case, Agent Brenneis

---

[6] The case of *United States v. Barrows*, *supra*, is somewhat inapposite, as it involved a law enforcement officer viewing first-hand pornographic images which the defendant, a municipal employee, had stored on his personal computer, where the computer was located at the defendant's workplace and had been networked to the city computer for the express purpose of file-sharing. In *Barrows*, the court held that, because the defendant had moved his personal computer into a public space and took no measures to protect its contents from public inspection, he lacked a reasonable expectation of privacy in the files that were viewed by the police officer. *See* 481 F.3d at 1249.

[7] As the Third Circuit Court of Appeals has explained,

> [t]he "standing" inquiry, in the Fourth Amendment context, is shorthand for the determination of whether a litigant's Fourth Amendment rights have been implicated. *See United States v. Kimball*, 25 F.3d 1, 5 (1st Cir.1994) ("We use the term 'standing' as a shorthand method of referring to the issue of whether the defendant's own Fourth Amendment interests were implicated by the challenged governmental action. 'Technically, the concept of "standing" has not had a place in Fourth Amendment jurisprudence for more than a decade, since the Supreme Court in *Rakas v. Illinois*, 439 U.S. 128, 99 S. Ct. 421, 58 L. Ed.2d 387 (1978), indicated that matters of standing in the context of searches and seizures actually involved substantive Fourth Amendment law.' *United States v. Sanchez*, 943 F.2d 110, 113 n. 1 (1st Cir. 1991).").

United States v. Mosley, 454 F.3d 249, 253 n. 5 (3d Cir. 2006).

[8] Some of the authority relied on by the Government implicitly suggests the contrary. Many of the cases cited by the Government involve situations like the case at bar where a law enforcement officer initially obtains remote access to the defendant's share pornographic files via P2P software and then uses this information as a basis to obtain a broader search warrant. While these cases generally recognize that no Fourth Amendment violation occurs by virtue of the law enforcement officer's warrantless, remote accessing of the defendant's shared files (or other publicly available information), several of these cases then go on to address probable cause challenges

could have entered the Defendant's home and downloaded from his computer any shared files without having first obtained any warrant at all. In short, even if the Defendant suffered no Fourth Amendment intrusion by virtue of Trooper Pearson's conduct in remotely accessing certain shared computer files, the Defendant nevertheless retained a reasonable expectation of privacy in his computer and his home such that he possesses "standing" to challenge the merits of the subject search.

B. *Probable Cause*

We turn next to the merits of the Defendant's suppression motion, which concerns the fundamental question whether the search warrant affidavit established probable cause to believe that evidence of a crime would be found on the Defendant's computer. The standards governing a probable cause determination are well-established:

> [t]he task of the issuing magistrate is simply to make a practical common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place, and the duty of a reviewing court is simply to ensure that the magistrate had a "substantial basis for ... concluding" that probable cause existed.

Illinois v. Gates, 462 U.S. 213, 238-39 (1983) (quoted in *United States v. Shields*, 458 F.3d 269, 277 (3d Cir. 2006) (ellipsis in the original)). In making this assessment, the affidavit is to be construed in its entirety and in a common sense and non-technical fashion. *Id.,* 462 U.S. at 230-31. Importantly, "[s]ufficient information must [have been] presented to the magistrate to allow that official to determine probable cause; his action cannot [have been] a mere ratification of the bare conclusions of others." *Id*. at 239. Accordingly, "a mere conclusory statement" in an affidavit "that gives the magistrate

---

to the broader search warrant without any reference to Fourth Amendment standing issues. *See, e.g., Stults*, 575 F.3d at 841-44; *Perrine*, 518 F.3d at 1204-05; *Borowy*, 577 F. Supp. 2d at 1137-38.

virtually no basis at all for making a judgment regarding probable cause" will not suffice. *Id*.

Here, the Defendant concedes that Agent Brenneis' affidavit supported a finding of probable cause to believe: (i) that the files which Trooper Pearson located through peer-to-peer networking were located on the Defendant's computer and (ii) that they matched the files in the Wyoming ICAC Task Force's national data base. "But what the affidavit fails to do," according to the Defendant, "is provide any information for [the issuing magistrate judge] to use to determine that there was a fair probability that those files were contraband or evidence of a crime." (Def.'s Mot. to Suppress [49] at p. 10.)

I do not agree that Agent Brenneis' affidavit was so deficient as to leave the magistrate judge without a substantial basis upon which to conclude that there was a fair probability that contraband or evidence of criminal activity would be found on the Defendant's computer. Here, two key pieces of information – *i.e.*, the highly graphic titles of the files which the Defendant was making available to other P2P users and Trooper Pearson's confirmation that these same files were among those identified by the Wyoming ICAC Task Force as "known child pornography" – provided a substantial basis for the magistrate judge's probable cause determination. The Defendant challenges the probative value of each of these two pieces of information.

(i) The Computer File Names

The Defendant vigorously disputes the idea that the titles of the 11 computer files could meaningfully inform the magistrate judge's probable cause analysis. He contends that, in order to find a fair probability that the files in question were contraband or evidence of a crime, the magistrate judge either had to view the files personally or have at her disposal (*i.e.*, contained within the affidavit) a sufficiently detailed description of the contents of the files as supplied by someone who had actually viewed them. Defendant argues that neither of these situations occurred here and, therefore, probable cause was lacking.

In the context of obscenity laws, the Supreme Court has stated that an issuing magistrate judge is not required to review the allegedly obscene material personally; rather, "a reasonably specific affidavit describing the content of a film generally provides an adequate basis for the magistrate to determine whether there is probable cause to believe that the film is obscene, and whether a warrant authorizing the seizure of the film should issue." *New York v. P.J. Video, Inc.*, 475 U.S. 868, 874 n.5 (1986). A number of federal courts have applied this principle in the context of child pornography cases. *See, e.g., United States v. Battershell*, 457 F.3d 1048, 1052 (9th Cir.2006) ("[A] judge may properly issue a warrant based on factual descriptions of an image."); *United States v. Chrobak*, 289 F.3d 1043, 1045 (8th Cir.2002) (ruling that a magistrate may base probable cause on viewing images or on a description of them); *U.S. v. Brunette*, 256 F.3d 14, 18 (1st Cir. 2001) ("A judge cannot ordinarily make this determination [whether an image constitutes child pornography] without either a look at the allegedly pornographic images, or at least an assessment based on a detailed, factual description of them.").

Here, as I have noted, the affidavit did not state that Trooper Pearson had personally viewed the files in question, nor did the affidavit provide a detailed recitation of what the files were observed to contain. The question therefore becomes whether the Magistrate Judge could draw a reasonable inference as to the probable content of the files based upon the highly descriptive names assigned to them.

Herein lies the central point of contention, for the Defendant strongly insists that the file names at issue in this case cannot support a finding of probable cause to believe that the files *actually contained* images of child pornography. He cites two reasons – one general, one specific – in support of this argument.

The Defendant's first reason for disputing the probative value of the file names is his assertion that, as a general proposition, file names are not a reliable indicator of the actual content of any given computer file obtained through P2P file sharing. He contends that the search warrant affidavit provides no information to establish that the

actual contents of files obtained through the use of peer-to-peer software correspond to their titles and, in fact, he extrapolates from the affidavit the opposite conclusion. He cites an article (apparently published by the "IEEE Computer Society" as part of the "Proceedings of the 41st Hawaii International Conference on System Sciences - 2008")[9] in support of the proposition that computer hackers will, in some instances, place malicious programs such as a virus, worm or spyware into a purposefully mislabeled file in order to infect and gain access to the searcher's computer. In fact, the Defendant suggested at oral argument, against the possibility that this Court might rely on the file names as an indicator of probable cause, that he would request an evidentiary hearing to establish as a factual proposition that file names do not necessarily correspond to actual file content. (*See* Tr. of 11/9/2009 Oral Argument [58] at pp. 25-27; 34-35.)

As is invariably the case, however, the ultimate determination as to whether an affidavit is supported by probable cause -- and the degree to which any particular factor may be relied on as an indicator of probable cause – depends on the specific facts at hand. *See Gates*, 462 at 232 ("[P]robable cause is a fluid concept-turning on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules."). That is no less true in the case at bar.

As a generic proposition, the Government would likely stipulate – and this Court would agree – that file names are not a definitive indication of actual file content and, therefore, only after downloading and viewing a particular file can one know with certainty whether the content of the file is consistent with its designated name. But "certainty has no part in a probable cause analysis." *U.S. v. Frechette*, 583 F.3d 374,

---

[9] *See* M. Eric Johnson, Dan McGuire, Nicholas D. Wiley, *The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users* (2008). We note that, generally, on review of an allegedly defective search warrant affidavit, courts are confined to an examination of the four corners of the affidavit and those reasonable inferences which arise from it, *U.S. v. Porter*, 438 F. Supp. 2d 554, 555 n.4 (E.D. Pa. 2006) (citing *United States v. Conley*, 4 F.3d 1200, 1204 (3d Cir.1993)), so it is questionable whether this Court is permitted to consider this information.

(6th Cir. 2009). On the contrary, "probable cause requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." *Illinois v. Gates*, 462 U.S. at 244 n.13.

Moreover, determining the existence (or lack) of probable cause involves making a "practical, common-sense decision" as to whether, given the totality of facts, a "fair probability" exists that contraband will be found in a particular place. *Gates*, 462 U.S. at 238. *See also United States v. Williamson,* 439 F.3d 1125, 1136 (9th Cir. 2006) ("[N]o more is required in issuance of a warrant than that the judge has made a 'practical, common-sense decision' that there was a 'fair probability' that actual child pornography would be found in the suspect's residence."); *United States v. Whitner*, 219 F.3d 289, 296 (3d Cir. 2000) (affidavit must be read in its entirety and in a commonsense and nontechnical manner).

As a matter of common sense, one can easily envision circumstances where a computer file name will fail to provide meaningful insight concerning specific file content, particularly if the file name involves a popular name or a term that is abstract, generic, or otherwise capable of differing interpretations. The Defendant postulates, for example, that:

> if the searcher is using the peer to peer software to search for music and wants to download Imagine by John Lennon he could use the search term Imagine or "John Lennon" and receive a list with hundreds of file names containing the term Imagine or "John Lennon." However, if the person downloads several of the files whose titles contain the search term, he might discover that a number of the files do not really contain the song Imagine by John Lennon but rather a different song altogether, or the song Imagine performed by an artist other than John Lennon, or a movie clip of John Lennon, or some content completely unrelated to the song Imagine or John Lennon. ...

(Def.'s Mot. to Supp. [49] at p. 2.) Clearly, a P2P file search conducted under the foregoing circumstances might well produce a large quantum of files whose titles fail to spell out the precise nature of their content. Thus, the Court is perfectly willing to credit the Defendant's hypothetical as far as it goes.

Moreover, the producer of a digital file is master of his own universe, so to

speak, and can choose to name his file anything his imagination can conceive. Therefore, common knowledge dictates that actual file content cannot be definitively determined from the file name alone. One individual's usage of a particular term might differ from another person's. Some words or phrases are inherently ambiguous. As one court has observed:

> ... the file name "Lolita,"... on its own could as easily reference an English term paper, a discussion of teacher-student relations, or contain adult or child pornography.[10] Likewise, in a vacuum, the title "Teen Angel" could as likely reference a popular 1960s song as it could be a video file containing child pornography. ...

United States v. Leedy, 65 M.J. 208, 215 (C.A.A.F. 2007). In addition, as the Defendant points out, computer hackers sometimes deliberately mislabel files with the goal of infecting an unsuspecting file sharer's computer.

However, it does not necessarily follow as an inevitable corollary from all of this that *no* file name can *ever* be regarded as a logical indication of the file's salient features. Just as one can envision circumstances where a particular file name might provide no basis for drawing inferences concerning the actual file content, one can also envision circumstances where the file name is so explicit and detailed in its description as to permit at least a reasonable inference as to what the actual file is likely to show. Many, if not most, of the files at issue here had titles that contained highly graphic references to specific sexual acts – including ejaculation, sexual intercourse, oral sex, and anal sex – involving children ranging in age from 7 to 13 years. Several of the files also reference terms such as "child_sex," "pedofilia," "illegal pedo sex," "incest," or "Lolita." The unmistakable inference which arises from such highly descriptive file names, is that the content includes material pertaining to the sexual exploitation of children – *i.e.*, evidence of criminal activity, if not outright contraband. Given the

---

[10] This Court notes that other appellate courts have recognized that the term "Lolita" is a "well-known moniker for minor girls," *United States v. Syphers*, 426 F.3d 461, 466 (1st Cir. 2005), and "often a code word for child pornography." *United States v. Grimes*, 244 F.3d 375, 379 n. 7 (5th Cir. 2001).

number of files in question and the pointed references in their titles to specific sexual acts involving young children – described in the most coarse and vulgar terms, this inference is a strong one.

The Defendant nevertheless reads the affidavit as supporting his proposition that the names of files obtained through P2P software cannot serve as meaningful indicators of the actual file content. He points in particular to the following paragraph in which Agent Brenneis discusses the utility of SHA1 values to law enforcement:

> SHA1 hash values are also extremely helpful to law enforcement because an investigator can be certain that an image being disseminated on the Gnutella network is child pornography simply by comparing that subject image's SHA1 hash value with a national database's listing of SHA1 hash values for known child pornography. This allows an extremely high degree of confidence that a known hash value represents a given file, in this case an image of child pornography, *regardless of the title utilized by the distributor or possessor of the image*.

(Brenneis Affidavit [49-2] at ¶ 17 (emphasis added).) According to the Defendant, this language demonstrates that "[t]he whole point of using the SHA1 hash value to identify files rather than file names is that the file names do not necessarily correspond to the file contents." (Def.'s Mot. to Supp. at 13.)

When considered in proper context however, the cited language merely establishes that use of SHA1 values provides an extremely high level of precision in identifying specific file content -- a level of precision which, according to the affidavit, is more unique than DNA matching. Such precision likely exceeds the exactitude necessary to establish proof beyond a reasonable doubt; certainly, it exceeds what is necessary under general probable cause standards. Thus, the affidavit may be fairly read as implying a fairly obvious principle – that SHA1 values provide a more reliable means of identifying actual file content than is possible by virtue of file names alone. This principle, however, does not lead ineluctably to the conclusion that file names thereby always constitute meaningless information.

On the contrary, a fair reading of the affidavit supports the relevance of the file

names in question. Agent Brenneis' affidavit discusses in some detail the process of peer-to-peer filing sharing and, in particular, the fact that users conduct searches for particular file content based on the use of keywords, which in turn produces a list of files in which the keyword appears. (*See* Brenneis Affidavit at ¶¶ 13-14.) For example,

> a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a search for files using a phrase such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed the files he/she wants to download. ...

(*Id*. at ¶ 14.)[11]

As a matter of common sense, the very fact that individuals utilize search terms with P2P software to produce results (i.e., ***file names***) consistent with their chosen search terms suggests a substantial degree of correlation between file names and file content; if file names were, as a general rule, completely random and bearing no relation whatsoever to their content, then there would be no point in conducting a search in the first place and the whole purpose of peer-to-peer file sharing would be frustrated because there would be no meaningful method for locating the sought-after file content. Here, the Magistrate Judge could logically infer that, by using search terms associated with child pornography, and in locating numerous files with names highly suggestive of such material, Trooper Pearson had probably been successful in identifying actual contraband.

In sum, I conclude that the extent to which a particular file name provides insight into the likely content of that file depends uniquely on the particular facts at hand. I also conclude that, at least in this case, it is a matter susceptible to a common sense

---

[11] As the Defendant explains it, "A person running peer to peer software can type in a search term and the software will then search the computers of all other individuals connected to the internet running the peer to peer software *for files with a file name that contains the search term. The software will then present the searcher with a list of files whose file names contained the search term."* (Def.'s Mot. to Suppress [49] at p. 2 (emphasis supplied).)

evaluation and not dependent upon expert testimony.

The Defendant maintains, however, that he is entitled to an evidentiary hearing on this point. Under *Franks v. Delaware*, 438 U.S. 154 (1978), a defendant is entitled to receive an evidentiary hearing upon request if he makes a substantial preliminary showing that the search warrant affidavit included a false statement, made knowingly and intentionally or with reckless disregard for the truth, which was material to a showing of probable cause. Here, however, there has been no preliminary showing of any false statement in the affidavit, nor does this Court perceive one; therefore, there is no occasion for an evidentiary hearing under *Franks*. Moreover, with regard to the Defendant's central thesis – that the titles or file names assigned by peer-to-peer users are not always a reliable indicator of what, exactly, is contained in the file – this Court has already accepted that premise as a matter of common sense, albeit one whose relevance in any given situation is highly fact-driven.

Defendant next argues that, regardless of the foregoing, the file names could not support a probable cause finding in this particular case because Agent Brenneis employed an improper, and unconstitutional, definition of "child pornography" in his affidavit. This point requires some background discussion.

In the section of his affidavit entitled "Statutory Basis," Agent Brenneis represented that the subject investigation is based on various provisions of 18 U.S.C.A. §§ 2252 and 2252A, which are part of the Child Pornography Prevention Act of 1996 (CPPA), 18 U.S.C.A. § 2251 *et seq.*. Section 2252 of the CPPA defines certain offenses in terms of activity involving visual depictions of minors engaging in "sexually explicit conduct," while § 2252A defines certain offenses in terms of activity involving "child pornography." *See generally* 18 U.S.C.A. §§ 2252 and 2252A and Brenneis Affidavit [49] at ¶5(a)-(e). The affidavit then goes on to provide the statutory definitions

of "sexually explicit conduct" (*see id*. at ¶ 5(f))[12] and "child pornography" (*see id*. at ¶ 5(g)), as (purportedly) set forth in 18 U.S.C.A. § 2256.

At issue here is the definition of "child pornography" which, according to Agent Brenneis' affidavit, is contained at 18 U.S.C.A. § 2256(8) and means:

> any visual depiction including any photograph, film, video, picture or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, [of] sexually explicit conduct, where:
>
> > (a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
> >
> > (b) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;
> >
> > (c) such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or
> >
> > (d) such visual depiction is advertised, promoted, presented, described or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

(Brenneis Affidavit at ¶ 5(g) (citing 18 U.S.C.A. § 2256(8)(A-D)).

As the Defendant points out, this definition comports with the version of § 2256(8) which was extant prior to the Supreme Court's decision in *Ashcroft v. Free*

---

[12] "Sexually explicit conduct" is statutorily defined as "actual or simulated":

> (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between person of the same or opposite sex;
>
> (ii) bestiality;
>
> (iii) masturbation;
>
> (iv) sadistic or masochistic abuse; or
>
> (v) lascivious exhibition of the genitals or pubic area of any person.

18 U.S.C.A. § 2256(2)(A). There is no contention here by the Defendant that the definition of "sexually explicit conduct" employed by Agent Brenneis differed in any material respect from this statutory definition or was otherwise inaccurate.

Speech Coalition, 535 U.S. 234 (2002). In *Free Speech Coalition*, the Supreme Court struck down as overbroad and unconstitutional two of the definitions of "child pornography" contained in Agent Brenneis' affidavit as set forth above in subsections (B) and (D).

Prior to *Free Speech Coalition*, the Supreme Court had held in *New York v. Ferber*, 458 U.S. 102 (1982), that pornography depicting actual minors falls outside the protection of the First Amendment and may therefore be lawfully prohibited regardless whether the images would be considered "obscene." *See generally Miller v. California*, 413 U.S. 15, 24-30 (1973) (discussing standards for determining "obscenity"). In *Free Speech Coalition*, the Court found that § 2256(8)(B) was unconstitutional because it covered material beyond the categories recognized as proscribable under *Ferber* and *Miller* and, in doing so, abridged the freedom to engage in a substantial amount of lawful speech. 535 U.S. at 256. The Court interpreted the statutory proscription of "any visual depiction" that is, "or appears to be," of minors engaging in sexually explicit conduct, as "captur[ing] a range of depictions, sometimes called 'virtual child pornography,' which include computer-generated images, as well as images produced by more traditional means." 535 U.S. at 241. This definition, the Court noted, prohibited a substantial amount of speech which might not necessarily appeal to the prurient interest or be patently offensive and which might well possess serious literary, artistic, political, or scientific value. *Id*. at 246. As examples of lawful speech which might be prohibited by the statute, the Court cited "a Renaissance painting depicting a scene from classical mythology" or movies filmed without any child actors wherein the actor "appears to be a minor" engaging in actual or simulated sexual intercourse. *Id*. at 241.[13]

In addition, the Court found § 2256(8)(D) to be overbroad and unconstitutional

[13] The Court expressed concern that modern productions of *Romeo and Juliet* or films such as *Traffic* and *American Beauty*, as well as countless others, might conceivably run afoul of the statute. *See* 535 U.S. at 247-48.

insofar as it proscribed sexually explicit materials that "conve[y] the impression" that minors are being depicted. *Free Speech Coalition*, 535 U.S. at 257. The Court noted that, "[e]ven if a film contains no sexually explicit scenes involving minors, it could be treated as child pornography if the title and trailers convey the impression that the scenes would be found in the movie." *Id*. Moreover, while the Court had previously recognized in *Ginzburg v. United States*, 383 U.S. 463, 474 (1966), that pandering may have evidentiary relevance bearing on the question whether particular materials are obscene, the *Free Speech Coalition* Court found that § 2256(8)(D) went beyond proscribing pandering by prohibiting the mere "possession of material described, or pandered, as child pornography by someone earlier in the distribution chain." *Id*. at 258. As the Court interpreted § 2256(8)(D), "[t]he provision prohibits a sexually explicit film containing no youthful actors, just because it is placed in a box suggesting a prohibited movie. Possession is a crime even when the possessor knows the movie was mislabeled." *Id*.

In short, the statutory language utilized by Agent Brenneis in his affidavit to give meaning to the term "child pornography" incorporates two definitions which have been found to be overbroad and unconstitutional by the Supreme Court. Given this fact, the Defendant reasons, the Magistrate Judge could not have found a fair probability that the content of the eleven files would contain actual contraband. While the Defendant concedes that "[t]he file names certainly present and describe the contents of the files in a manner that *convey the impression* that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct," (Def.'s Supp. Motion at p. 14 (emphasis supplied)), he argues that this is no longer a legitimate basis for classifying material as prohibited child pornography. In other words, the argument goes, the magistrate judge here had no basis for determining that the eleven files located by Trooper Pearson contained child pornography involving the use of actual minors, as opposed to something more innocent. For all the Magistrate Judge knew, the Defendant posits, the actual content of the eleven files could have involved only images

of actors who were over the age of 18 but appeared to be minors engaging in sexually explicit conduct or material that included no such images but which had merely been pandered as involving minors engaged in sexually explicit conduct.

It bears repeating, however, that our enterprise at this juncture is concerned only with fair probabilities, not with certainties, nor proof beyond a reasonable doubt, nor even *prima facie* evidence of criminal activity. *See Illinois v. Gates*, 462 U.S. at 235. Moreover, it involves viewing the evidence at hand in a "practical, nontechnical" sense. *Id.* at 231. As the Supreme Court has explained:

> Long before the law of probabilities was articulated as such, practical people formulated certain common-sense conclusions about human behavior; jurors as factfinders are permitted to do the same – and so are law enforcement officers. Finally, the evidence thus collected must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement.

Id. at 231-32.

Given the highly descriptive titles of the computer files at issue, it would be entirely logical for a magistrate judge to find a fair probability that the actual file content would contain contraband (*i.e.*, images involving the sexual exploitation of real children), as opposed to constitutionally protected speech. That the file titles bespeak content of a graphic sexual nature is not seriously disputed by the Defendant. The fact that many of the titles explicitly reference the involvement of children ranging in ages from 7 years to 14 years makes it less likely that the true content would involve actors of majority age. In addition, the fact that certain file names referred to the children by name (e.g., "14yo Isabel" and "Jessica 11yo") permits a reasonable inference that identifiable minors were used in the actual images. The other possibility – that the content might have involved sexual images of minors produced through the use of computer morphing – is of no obvious benefit to the Defendant. As the Supreme Court has explained, computer morphing involves a process whereby pornographers, "[r]ather than creating original images, ... can alter innocent pictures of real children so that the children appear to be engaged in sexual activity." *Free Speech Coalition*, 535 U.S. at

242. The Court has noted that, "[a]lthough morphed images may fall within the definition of virtual child pornography, they implicate the interests of real children and are in that sense closer to the images in *Ferber*." *Id*. Such images are proscribed under the language of 18 U.S.C.A. § 2256(8)(C), which the Supreme Court did not address in *Free Speech Coalition*, and which stands as a currently valid proscription on virtual child pornography under the definition utilized by Agent Brenneis.

Furthermore, the warrant also sought evidence concerning possible violations of 18 U.S.C.A. § 2252, which concerns visual depictions that involve the use of minors engaging in "sexually explicit conduct." "Sexually explicit conduct" is, in turn, defined partly in terms of specific actual or simulated sexual acts, including masturbation or "sexual intercourse – including genital-genital, oral-genital, anal-genital or oral-anal," irrespective of whether it involves persons of the same or opposite sex. 18 U.S.C.A. § 2256(2)(A)(i) and (iii). Based on the file names in question, the Magistrate Judge could have found a fair probability that a search of the Defendant's computer would reveal evidence of minors engaged in sexually explicit conduct.[14]

In sum, given the unique facts of this case, the Magistrate Judge was entitled to infer from the highly descriptive and graphic file names and the other information presented in the affidavit that there was a fair probability that the Defendant's computer would contain material prohibited under either 18 U.S.C.A. § 2252 or § 2252A. The fact that the file names were not conclusive proof of their content, and the fact that actual

---

[14] The Defendant insists that we cannot consider this theory because the affidavit averred only that the content of the files was "child pornography." However, both the warrant and supporting affidavit clearly reference the fact that evidence was being sought relative to visual depictions of minors engaged in "sexually explicit conduct" that might violate 18 U.S.C.A. § 2252(a). (*See, e.g.,* Search Warrant [49-2] at pp. 2-4 and supporting affidavit at ¶¶ 2, 5(a), (b), (c), (f).) Moreover, the definition of "child pornography," for purposes of establishing a violation of 18 U.S.C.A. § 2252A, incorporates the concept of minors engaged in sexually explicit conduct. *See* 18 U.S.C.A. § 2256(8) and Brenneis Affidavit at ¶ 5(g). Accordingly, to the extent material is classified as "child pornography" within the meaning of § 2256(8), it necessarily involves depictions of minors engaging in "sexually explicit conduct."

content could only be ascertained with certainty upon a viewing of the files, does not change this result. Once again, we are concerned only with fair probabilities and, more specifically, whether the Magistrate Judge had a substantial basis for finding a fair probability that evidence of criminal activity would be found on the Defendant's computer. In making her probable cause determination, the Magistrate Judge was not required to rule out all other possible inferences as to the content of the eleven files, particularly where the most logical inference pointed to unlawful content.[15] *See, e.g., United States v. Carmel*, 548 F.3d 571, 576 (7th Cir. 2008) (defendant's possession of top handles, which could potentially be utilized in both lawful and unlawful weapons, supported finding of probable cause to believe that defendant possessed unregistered machine gun; the potential lawful use of the top handles did not negate the other incriminatory inference); *United States v. Colquitt*, No. 07-CR-55, 2007 WL 4305551 at *7 (E.D. Wis. Dec. 7, 2007) (competing inferences arising from affidavit as to whether evidence of child pornography would be found on the defendant's home computer did

---

[15] The Court notes that, in the wake of *Ashcroft v. Free Speech Coalition*, *supra*, Congress enacted the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act ("PROTECT Act"), which amended the definition of "child pornography" formerly contained in 18 U.S.C.A. § 2256(8)(B) and which repealed the definition contained in § 2256(8)(D). *See* Pub. L. No. 108-21 (April 30, 2003), § 502(a)(1), (a)(3); 18 U.S.C. § 2256(8)(B). In conjunction with the passing of the PROTECT Act, Congress made express findings concerning the child pornography trade including, among others, the following:

> (7) There is no substantial evidence that any of the child pornography images being trafficked today were made other than by the abuse of real children. ...
>
> ***
>
> (11) Leading experts agree that, to the extent that the technology exists to computer generate realistic images of child pornography, the cost in terms of time, money, and expertise is – and for the foreseeable future will remain – prohibitively expensive. As a result, for the foreseeable future, it will be more cost-effective to produce child pornography using real children. ...

Pub. L. No. 108-21, § 501 Findings, 117 Stat. 650, 677-78.

not defeat issuing authority's finding of probable cause).

(ii) The WICAC Task Force Information

The second piece of information supporting the Magistrate Judge's probable cause determination is Agent Brenneis' representation that the SHA1 values of the eleven shared files "matched the SHA1 values of files in the Wyoming Internet Crimes Against Children (ICAC) Task Force's national [database] of SHA1 values for known child pornography computer files." (Brenneis Affidavit at ¶ 23.) The Defendant contends that this information is insufficient in that the affidavit gives no description of the content of the files from the Wyoming ICAC Task Force database that would explain how that entity determined that its "known" files are in fact child pornography, nor is any explanation given as to what the Wyoming ICAC Task Force is or how it has the expertise to determine what is or is not child pornography.

I first consider the affidavit's lack of detail concerning the Wyoming ICAC Task Force. The Defendant suggests this is fatal because, for all the Magistrate Judge knew, the Task Force could have been some self-appointed group of private citizens with no particular expertise in evaluating what constitutes child pornography.

I am not persuaded, however, that the Magistrate Judge was left without any basis whatsoever for determining the reliability of the information pertaining to the Wyoming ICAC Task Force. Judicial officers reviewing search warrant applications are entitled to draw reasonable inferences from the information contained in the supporting affidavit, *see United States v. Wallace*, 550 F.3d 729, 732 (8th Cir. 2008), and the very name "Wyoming Internet Crimes Against Children Task Force" connotes a state-authorized law enforcement body possessing particular expertise relevant to "internet crimes against children."[16] In fact, the term "task force" is commonly understood to

[16] In any event, magistrate judges passing on warrant applications are permitted to take judicial notice of adjudicative facts which are not subject to reasonable dispute. *See United States v. Ellsworth*, 647 F.2d 947, 963 (9th Cir. 1981), *United States v.*

mean, among other things, a body possessing special expertise on a particular subject matter. *See Dictionary.Com* (defining "task force" as "a group or committee, usually of experts or specialists, formed for analyzing, investigating, or solving a specific problem") (available at "http://dictionary.reference. com/browse/task+force") (citing the Random House Dictionary, 2009). Moreover, as a law enforcement body, the Task Force could generally be regarded as a reliable source of information. *See U.S. v. Lapsins*, 570 F.3d 758, 764 (6th Cir. 2009) ("[I]n general, 'another law enforcement officer is a reliable source and ... consequently no special showing of reliability need be made as a part of the probable cause determination.'") (citing 2 Wayne R. LaFave, Search and Seizure §3.5(a) (4th ed.2008)).

The Defendant objects that the affidavit provides no information as to how or

---

Sevier, 439 F.2d 599, 603 (6th Cir. 1976). *See also* Fed. R. Evid. 201(b) ("A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court *or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned*.") (emphasis added). The Wyoming ICAC Task Force's identity as one of many regional law-enforcement agencies comprised of state and federal agents and supported by the United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention – is both readily ascertainable and not subject to any reasonable dispute. According to the Wyoming Attorney General's website, the Task Force is organized under the Wyoming Division of Criminal Investigation. Further,

> The ICAC Team is located in Cheyenne, WY and is comprised of five (5) Special Agents, one Immigration and Customs Enforcement Agent and one Federal Bureau of Investigations Agent. The ICAC team concentrates on the use of the Internet to exploit children. The agents are trained in Internet undercover operations as well as computer forensic examinations. The team is partially funded by the Office of Juvenile Justice and Delinquency Prevention.

See "http://attorneygeneral.state.wy.us/dci/about.html." *See also* Internet Crimes Against Children Task Force Training & Technical Assistance Program ("About Us") (located at "http://www.icactraining.org/ About.htm"); Wyoming Attorney General, Division of Criminal Investigation - Overview (located at "http://attorneygeneral.state.wy. us/dci/about.html").

why the Task Force categorized the files in question as "known child pornography." According to the Defendant, we should assume the Task Force employed the same overly broad definition of "child pornography" set forth in the affidavit. Thus, the Defendant argues, as far as the Magistrate Judge knew, the Task Force member who made the determination that the images in the national database were "child pornography" could have believed that the images at issue here involved youthful looking actors who were over the age of 18 who "appeared to be" minors engaging in sexually explicit conduct, or they could have believed that the material was otherwise lawful but merely being pandered as images involving minors engaging in sexually explicit conduct.

As an initial matter, it is not clear to this Court that the errant definition of "child pornography" incorporated into the affidavit should logically be attributed to the presumably independent determination made by the Task Force that particular computer files constitute child pornography. In any event, however, assuming *arguendo* that the reviewing Magistrate Judge was required to presume that the WICAC Task Force would have utilized the same overly broad definition of "child pornography" as was set forth in the affidavit, it does not follow that probable cause is lacking. I have previously determined that, considering the names of the files in question, the Magistrate Judge could logically infer that the content of the files probably contained images of "child pornography" as that term is currently (and legally) defined – *i.e.*, depictions of actual children engaged in sexually explicit conduct and/or depictions created, adapted or modified to appear that identifiable minors are engaging in sexually explicit conduct. That being the case, the Magistrate Judge could have likewise assumed that the Wyoming ICAC Task Force had categorized the files as "child pornography" because their actual content satisfied one or more of those same criteria.

The Defendant makes the further point that, even if we assume that whomever made the determination that the images in the Task Force's database were child pornography did so based on the valid definitions of "child pornography" contained in

the affidavit, *i.e.*, 18 U.S.C.A. § 2256(8)(A) and (C), the affidavit still fails to establish probable cause because it simply states in conclusory fashion that someone else – *i.e.*, the Task Force – has determined that the images in the database are "child pornography." Thus, Defendant reasons, the Magistrate Judge had no independent basis from which to make her own probable cause determination; instead, she merely ratified the determination of another entity. In support of this conclusion, the Defendant relies upon *United States v. Diyn*, Criminal No. 3:2006-37, 2008 WL 2795942 (W.D. Pa. July 18, 2008), wherein the court found that "the conclusions of [the National Center for Missing and Exploited Children ("NCMEC")] that the two images in question were 'both confirmed child pornography' certainly does not establish probable cause." *Diyn, supra* at *6. The court explained that, "[a] nude picture of a minor is not per se violative" of Pennsylvania and federal child pornography laws and "it is unknown from the affidavit of probable cause that NCMEC ... made its evaluation of the images in conformity with what is outlawed by the Pennsylvania statute." *Id*. at *6. "Without further explanation," the court found, "NCMEC's conclusion that matter is 'child pornography' can include a wide spectrum of images that are both legal and illegal under the Pennsylvania law and such a conclusion cannot form the basis for a determination of probable cause." 2008 WL 2795942 at *6 n. 7.

In assessing probable cause, however, we are not permitted to view one piece of information in isolation but must consider, instead, the totality of information contained in the affidavit. *United States v. Whitner*, 219 F.3d at 296 ("[S]tatements in an affidavit may not be read in isolation – the affidavit must be read as a whole.") (alteration in the original) (citation omitted). Here, there is more in the affidavit than simply the conclusory determination by another entity (albeit one that ostensibly possesses special expertise in the area of internet crimes against children) that the images in question constitute "child pornography." In addition to the Wyoming ICAC Task Force's confirmation that the files in question constituted known child pornography, the Magistrate Judge could consider the fact that Trooper Pearson had conducted a peer-

to-peer search using terms associated with child pornography and had located on the Defendant's computer numerous files whose titles contained highly graphic references to specific sexual acts involving prepubescent minors and which included terms such as "child_sex," "incest," "illegal pedo sex," "pedofilia," and "Lolita." Thus, the Magistrate Judge could infer that the Wyoming ICAC Task Force had classified the files as "child pornography" because they contained depictions of minors engaging in sexually explicit conduct for purposes of 18 U.S.C.A. § 2256(8)(A), or depictions that had been "created, adapted, or modified to appear" as though identifiable minors were engaging in sexually explicit conduct for purposes of § 2256(8)(C).

In sum, based upon the totality of circumstances presented in Agent Brenneis' affidavit, the Magistrate Judge had a substantial basis from which to find a fair probability, or a "substantial chance," that material in violation of 18 U.S.C.A. § 2252 and/or §2252A would be found on the Defendant's computer. Accordingly, neither the fruits of Agent Brenneis' search, nor the Defendant's subsequent statements, need be suppressed.

C. *Good Faith*

Finally, even if the affidavit did not establish probable cause to believe that contraband or evidence of a crime would be found on the Defendant's computer, the Court would find that the good faith exception to the exclusionary rule, as set forth in *United States v. Leon*, 468 U.S. 897 (1984), is applicable here. Pursuant to the good faith exception, suppression "is inappropriate when an officer executes a search in objectively reasonable reliance on a warrant's authority." *United States v. Williams*, 3 F.3d 69, 74 (3d Cir.1993). "The test for whether the good faith exception applies is 'whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.'" *United States v. Loy*, 191 F.3d 360, 367 (3d Cir.1999) (quoting *Leon*, 468 U.S. at 922 n. 23).

Under Third Circuit precedent, the mere "fact that an officer executes a search

pursuant to a warrant typically suffices to prove that an officer conducted a search in good faith and justifies application of the good faith exception." *United States v. $92,422.57*, 307 F.3d 137, 146 (3d Cir.2002) (internal quotation omitted). However, the Circuit has identified four situations in which suppression is appropriate – *to wit*, situations where:

> (1) the magistrate issued the warrant in reliance on a deliberately or recklessly false affidavit;
>
> (2) the magistrate abandoned his judicial role and failed to perform his neutral and detached function;
>
> (3) the warrant was based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; or
>
> (4) the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized.

Williams, 3 F.3d at 74 n. 4 (internal citations and quotation omitted).

Here, the Defendant argues only the third exception – that the warrant affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." He essentially faults the executing officers in two respects. For one, he argues, any reasonably well-trained officer would have known that the affidavit was legally deficient in that it lacked a detailed, factual description of the images depicted in the eleven computer files. For another, he argues, good faith cannot be found to exist where the affidavit incorporates an unconstitutional definition of the term "child pornography."

I have already determined that, when read in a holistic, non-technical, and common sense fashion, the affidavit provided the issuing Magistrate Judge a substantial basis for her determination that there was a fair probability, *i.e.,* a "substantial chance," of finding material on the Defendant's computer in violation of 18 U.S.C.A. § 2252 or 2252A. The fact that eleven files located on the Defendant's files had been among those catalogued by the Wyoming ICAC Task Force as "known child pornography," coupled with the fact that the eleven file names included terms such as

"pedofilia," "illegal pedo sex," "incest," "Lolita," and "child_sex" and referenced acts of ejaculation, cunnilingus, sexual intercourse, incest, and fellatio involving young children, provided ample ground to support an objectively reasonable assumption by Agent Brenneis that probable cause had been established.

The Defendant insists that no good faith could exist here, however, because Agent Brenneis' affidavit included a definition of "child pornography" which has been struck down, in part, by *Ashcroft v. Free Speech Coalition*. The Defendant notes that good faith may shield an officer where the officer acts in reliance on a statute which is subsequently found to be unconstitutional, *see Illinois v. Krull*, 480 U.S. 340 (1987), but, he insists, "it is beyond dispute that good faith does not exist when a police officer relies on a statute that the Supreme Court has found unconstitutional six years earlier and which no longer is present in the United States Code." (Def.'s Mot. to Supp. at 21.) In support of this principle the Defendant cites *Ryan v. County of DuPage*, 45 F.3d 1090, 1094 (7th Cir. 1995) ("If there is probable cause to believe that the defendant has committed a crime by violating some rule, the rule's invalidity, while a defense to a conviction for the crime, is not a ground for his challenging the arrest for violating the rule under the Fourth Amendment, ... unless the invalidity of the rule was or should have been plain to the arresting officers.") (internal citations omitted); and *Buffkins v. City of Omaha, Douglas County, Neb.*, 922 F.2d 465 (8th Cir. 1990) (arrest made pursuant to unconstitutional city ordinance, which City had failed to repeal, violated Fourth Amendment).

This principle has relevance where there is no valid basis for finding probable cause absent reliance on an unconstitutional law. That is not the case here, however. For the reasons I have previously discussed, probable cause existed to believe that the Defendant had on his computer materials depicting minors engaged in sexually explicit conduct, within the meaning of 18 U.S.C.A. § 2256(2)(A) and/or material which constituted "child pornography" within the meaning of 18 U.S.C.A. § 2256(8)(A) or (C), either of which would have violated federal law. *See* 18 U.S.C.A. §§ 2252 and 2252A.

At the very least, a reasonably well-trained officer could have believed that there was adequate probable cause to support the search, notwithstanding the unconstitutional provisions that were included in the affidavit.

The Defendant criticizes this line of analysis on the ground that we cannot know the Magistrate Judge's subjective intent in approving the warrant and, therefore, he believes, the entire warrant must fail. But the concept of probable cause is generally understood to be an objective one in the sense that a reviewing court "must determine only that the magistrate judge had a 'substantial basis' for concluding that probable cause existed to uphold the warrant." *Whitner*, 219 F.3d at 296 (quoting *Gates*, 462 U.S. at 238). In determining whether a "substantial basis" exists for the magistrate judge's decision, we recall that the task of the issuing magistrate judge is simply to "make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him ... there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id*. (quoting *Gates*, 462 U.S. at 238). Accordingly, even assuming that the Magistrate Judge subjectively relied on an unconstitutional definition of "child pornography" in issuing the warrant, it is of no legal moment because the affidavit supplied a sufficient legal basis for establishing probable cause on valid, independent grounds.

Defendant interprets the cases following *New York v. P.J. Video, Inc.*, *supra*, as establishing the rule that "a search warrant in child pornography cases must provide at least **some** description of the alleged images of child pornography." (Def.'s Mot. to Supp. [49] at p. 17 (citing *P.J. Video, Inc.; United States v. Christie*, 470 F. Supp. 2d 756, 689 (D.N.J. 2008), and *United States v. Diyn*, No. Crim. 3:2006-37, 2008 WL 2795942 (W.D. Pa. Jul. 18, 2008)) (emphasis in the original). The purpose of this requirement, as he notes, is to prevent the Magistrate Judge from being a "rubber stamp" for law enforcement. (*Id*. at p. 16.) The Defendant apparently interprets my recent ruling in *United States v. Dennington*, No. 1:07-cr-43-SJM-1, 2009 WL 2591763 at *24 (W.D. Pa. Aug. 21, 2009) as declining to recognize this principle. (Def.'s Mot. to

Supp. [49] at pp. 16-17.)

It should be noted, however, that *Dennington* was concerned with the sufficiency of an affidavit in the particular factual context of child pornography defined in terms of the alleged "lascivious exhibition of the genitals or pubic area" of a minor. *See* 18 U.S.C.A. § 2256(2)(A)(v). The specific point raised by the defense in *Dennington* was whether the affidavit had provided sufficiently descriptive language to the issuing magistrate judge where the affidavit stated that an investigating officer had observed and downloaded from a particular website numerous images which she felt "depicted minors engaged in a lascivious display of their genitalia." *Id*. at *20 (quoting the affidavit). The Defendant relied heavily on the rulings in *Brunette*, 256 F.3d 14, 17-18 (1st Cir. 2001) and *Battershell*, 457 F.3d 1048, 1051 (9th Cir. 2006), as establishing the rule that it is critical to supply the issuing magistrate a detailed description of the content of an alleged "lascivious display" image because the concept of "lasciviousness" is highly subjective and inherently imprecise. (Def.'s Mot. to Suppress [62] at p. 17 (arguing that the failure to supply the issuing magistrate with the actual images or a detailed factual description of the images is "fatal" when the images are alleged to depict minors engaging in the lascivious display of their genitalia "because the phrase 'lascivious exhibition of the genitals' is not self-defining" (citing *United States v. Villard*, 885 F.2d 117 (3d Cir. 1989).) *See also Brunette*, 256 F.3d at 18 (noting that "'the identification of images that are lascivious will almost always involve, to some degree, a subjective and conclusory determination on the part of the viewer,'" and "[t]hat inherent subjectivity is precisely why the determination should be made by a judge, not an agent.") (citation omitted); *Battershell*, 457 F.3d at 1053 (contrasting other, more concrete definitions of "sexually explicit conduct" with the "lascivious display" definition and noting that "the more demanding standard for establishing probable cause" as annunciated in *Brunette* does not apply in non-"lascivious" cases).

In *Dennington*, this Court opined that the rule of *Brunette* and *Battershell* was not necessarily the well-settled law in this circuit, at least as of 2006. The Court also

observed that those cases had not necessarily been viewed as well-settled law by courts of other circuits:

> One district court has interpreted *Brunette* as "prohibit[ing] the issuance of a search warrant for child pornography without an independent review by the judge of the images used to establish probable cause or without a minutely detailed (read lurid) description of those images by the police officer." *United States v. Grant*, 434 F. Supp. 2d 735, 746 (D. Neb.2006). The Grant court went on to reject *Brunette* on the ground that it conflicted with controlling circuit law, and it cited *United States v. Chrobak*, 289 F.3d 1043, 1045 (8th Cir.2002), for the controlling rule that an affidavit is "sufficient when it recite[s] the language of the statute, such as 'graphic files depicting minors engaged in sexually explicit conduct.' " (Here, the search warrant affidavit's description of the images copied from [the allegedly pornographic website] tracked the statutory "lascivious" language that is used to describe "sexually explicit conduct" [ ] which, in turn, is one term used to describe "child pornography." *See* 18 U.S.C. § 2256(8).) A different district court from the Second Circuit, commenting on the rule of *Brunette* and *Battershell*, has observed that "the requirement that, in the lasciviousness context, law enforcement officials append to the warrant affidavit, or include therein a reasonably detailed description of, the allegedly proscribed material is relatively new and, at least within the Second Circuit, "unclear." *United States v. Genin*, 594 F. Supp. 2d 412, 426 (S.D.N.Y.2009) (upholding search on good faith grounds where affidavit contained agent's bare conclusion that videos contained "child pornography") (citing *United States v. Jasorka*, 153 F.3d 58 (2d Cir.1998)). *See also United States v. Simpson*, 152 F.3d 1241, 1246-47 (10th Cir.1998) (where affidavit neither presented to the issuing judge copies of unlawful materials believed to be in the defendant's possession, nor described in detail the content of those materials, but merely informed the judge that the material was "child pornography," the information in affidavit was nevertheless sufficient for the judge to find probable cause for the search).

Dennington, supra, at *24 (internal footnote omitted).

In citing this authority, this Court was not denying the viability of the principle announced in *P.J. Video, Inc.*. Rather, the Court was simply attempting to illustrate the point that courts which have endeavored to apply that principle in the context of child pornography cases have arrived at somewhat differing – and highly fact-driven – conclusions concerning the level of description that is necessary to permit the magistrate judge to make an independent evaluation of probable cause. *See, e.g.*, *United States v. Gatherum*, No. 08-4683, 2009 WL 1931229 at * 5 (4th Cir. July 7, 2009) (affidavit which stated that the subject images depicted a minor engaged in "sexually explicit behavior," and which included the relevant statutory definition of "sexually

explicit conduct," was sufficient and consistent with the type of language which other courts have found to be sufficient to establish probable cause) (citing cases); *United States v. Battershell*, 457 F.3d 1048 (9th Cir. 2006) (officer's description of picture showing prepubescent female naked in bathtub did not establish probable cause to believe that picture contained the lascivious exhibition of a minor's genitals, but description of second photo as depicting another young female having sexual intercourse with an adult male provided probable cause to believe that the image involved minors engaged in sexually explicit conduct); *United States v. Chrobak*, 289 F.3d 1043, 1045 (10th Cir. 2002) (affidavit sufficient where officer described images as "graphic files depicting minors engaged in sexually explicit conduct"); *United States v. Brunette*, 256 F.3d 14, 17 (1st Cir. 2001) (affidavit, which asserted merely that images linked to the defendant depicted "a prepubescent boy lasciviously displaying his genitals," was insufficient to establish probable cause, absent any descriptive support and without an independent review of the images, but search upheld on good faith grounds); *United States v. Diyn, supra*, at *7 (affidavit, which described images as ones that "appear to involve child pornography" and depicting "young female children between the ages of 7 and 12 in various states of undress" was sufficient to adequately represented that the images involved nudity of a nature intended "for the purpose of sexual stimulation or gratification or any person who might view such depiction" in violation of 18 Pa. C.S.A. § 6312(a)); *United States v. Grant*, 434 F. Supp. 2d 735, 746 (D. Neb. 2006) (affidavit which stated that computer repairman claimed to have seen "child pornography" on a computer was sufficient to establish probable cause).

In this case, I do not believe that the rule of *P.J. Video* was violated, much less violated in a manner obvious to any well-trained officer. The Magistrate Judge here was aware that the actual content of the Defendant's files had been classified as "known child pornography" by the Wyoming ICAC Task Force, and the highly descriptive names of those files provided the Magistrate Judge a logical basis for inferring what the actual content would depict and why the content had been classified

as child pornography. Thus, notwithstanding the authority relied upon by the Defendant, I conclude that a reasonably well-trained officer could hold a sincere and objectively reasonable, good faith belief that the information in the affidavit provided the Magistrate Judge with an adequate basis for making an her own independent determination that a search of the Defendant's computer would probably turn up evidence of unlawful material.

The Court recognizes that the Defendant has taken strong exception to the idea that the eleven file names at issue could serve as a sufficient indication of their probable content. Other courts have recognized, however, that file names and like evidence may have probative value in a probable cause determination. *See, e.g., United States v. Eichert*, 168 Fed. Appx. 151, 152, 2006 WL 279019 at ** 1 (9th Cir. Feb. 3, 2006) (issuing judge had substantial basis for probable cause finding where affidavit stated that defendant's computer screen displayed about 100 newsgroup listings, including newsgroups regarding "teens, preteen, sex, children and young girls," and his computer hard drives and storage media contained files whose titles referenced girls' names and terms such as "teens, too young, early teens, preteens," and sex words); *United States v. Roller*, No. CR-08-00361-RMW, 2009 WL 3762417 at * 4 (N.D. Cal. Nov. 9, 2009) (affidavit supplied sufficient factual basis to assert that website to which defendant purchased access was a child pornography website; apart from three images described in the affidavit, "[s]ome of the titles of the subject identifiers by their titles alone" suggested child pornography (e.g. "Underage Home," "Spycam Lolitas," "Kidz Index")); *United States v. Borowy*, 577 F. Supp. 2d 1133, 1138 (D. Nev. 2008) (finding that file name entitled "CPTVG 13 bond 10-11-12yo Childlover little collection video39girl" and others detected on the defendant's computer through a P2P file sharing program were named in such a way as to suggest that the files contained child pornography; these filenames alone provided the magistrate probable cause to issue a warrant even without reference to their content). *Accord United States v. Leedy*, 65 M.J. at 214-16 (magistrate properly found probable cause to search defendant's

computer for child pornography where defendant's roommate reported that he had observed play list of files displayed on the defendant's computer with titles that roommate perceived as describing pornographic material, including one named "three black guys and one white girl," and these files appeared alongside another file named "14 year old Filipino girl").

Finally, the Court notes the Supreme Court's admonition in *Herring v. United States*, --- U.S. ----, 129 S. Ct. 695, 172 L. Ed.2d 496 (2009), that, to justify application of the exclusionary rule, "the benefits of deterrence must outweigh the costs." *Id.* at 700. As the Court explained:

> [t]he principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free-something that "offends basic concepts of the criminal justice system." *Leon, supra*, at 908, 468 U.S. 897, 104 S. Ct. 3405, 82 L. Ed.2d 677. "[T]he rule's costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application." *Scott, supra*, at 364-365, 524 U.S. 357, 118 S. Ct. 2014, 141 L. Ed.2d 344 (internal quotation marks omitted); *see also United States v. Havens*, 446 U.S. 620, 626-627, 100 S. Ct. 1912, 64 L. Ed.2d 559 (1980); *United States v. Payner*, 447 U.S. 727, 734, 100 S. Ct. 2439, 65 L. Ed.2d 468 (1980).

129 S. Ct. at 701. "To trigger the exclusionary rule," the Court wrote, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id*. at 702. Thus, the rule is best suited to deter "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.*

To the extent probable cause could be found lacking in Agent Brenneis' affidavit, the degree of police misconduct involved fails to rise to the level necessary to justify application of the exclusionary rule. Though the Defendant would likely characterize Agent Brenneis' reference to two unconstitutional statutory provisions as reckless, or at the very least, grossly negligent conduct, his culpability must be judged not by that conduct alone but by reference to his reliance on the warrant as a whole. For the reasons previously stated, I conclude that Agent Brenneis did not act recklessly or in a grossly negligent manner in presuming the warrant's validity. Nor am I persuaded,

under the circumstances here, that the benefits which would result from the deterrence of Agent Brenneis' alleged misconduct would outweigh the costs.

In sum, I conclude that Agent Brenneis' affidavit contains sufficient evidence to warrant a sincerely held and objectively reasonable belief that a fair probability existed that materials in violation of 18 U.S.C.A. §§ 2252 and/or 2252A would be found on the Defendant's computer. Given the unique facts of this case, this Court cannot conclude that the warrant so lacked the requisite indicia of probable cause that it was "entirely unreasonable" for an official to believe otherwise.

III. CONCLUSION

Based upon the foregoing reasons, the Defendant's motion to suppress will be denied. An appropriate order follows.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA,	)	
	)	Case No. 1:08-cr-51-SJM
v.	)	
	)	
ROBERT EUGENE BEATTY	)	

O R D E R

AND NOW, *to wit*, this 31st day of December, 2009, for the reasons set forth in the accompanying Memorandum Opinion,

IT IS HEREBY ORDERED that the Defendant's Motion [49] to Suppress Evidence is DENIED.

s/ Sean J. McLaughlin

SEAN J. McLAUGHLIN
United States District Judge

cm: All counsel of record.